QUALYS SECURITY CONFERENCE 2018

Vers une nouvelle approche de la Sécurité des conteneurs

Leif Kremkow
Directeur Technique, Qualys

Agenda

Containers and DevOps

Your responsibility

Customer Case Studies

Container Lifecycle Challenges

Use Cases & Demo

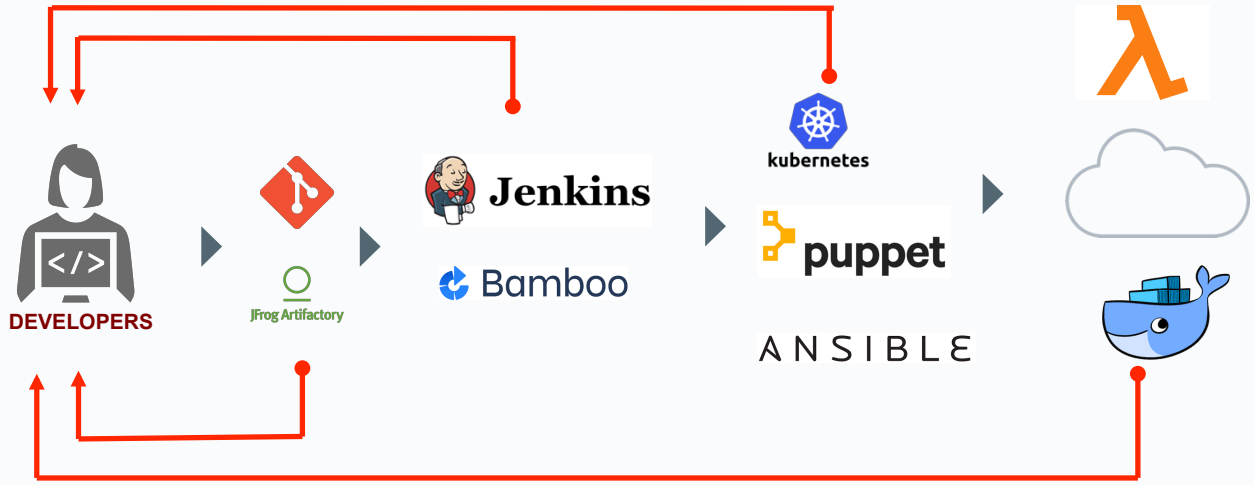
Everybody Loves Containers

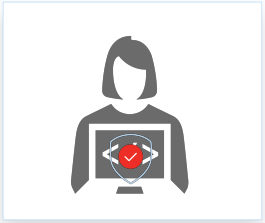
Portability

Agility

Density

DevOps/DevSecOps Requirements…



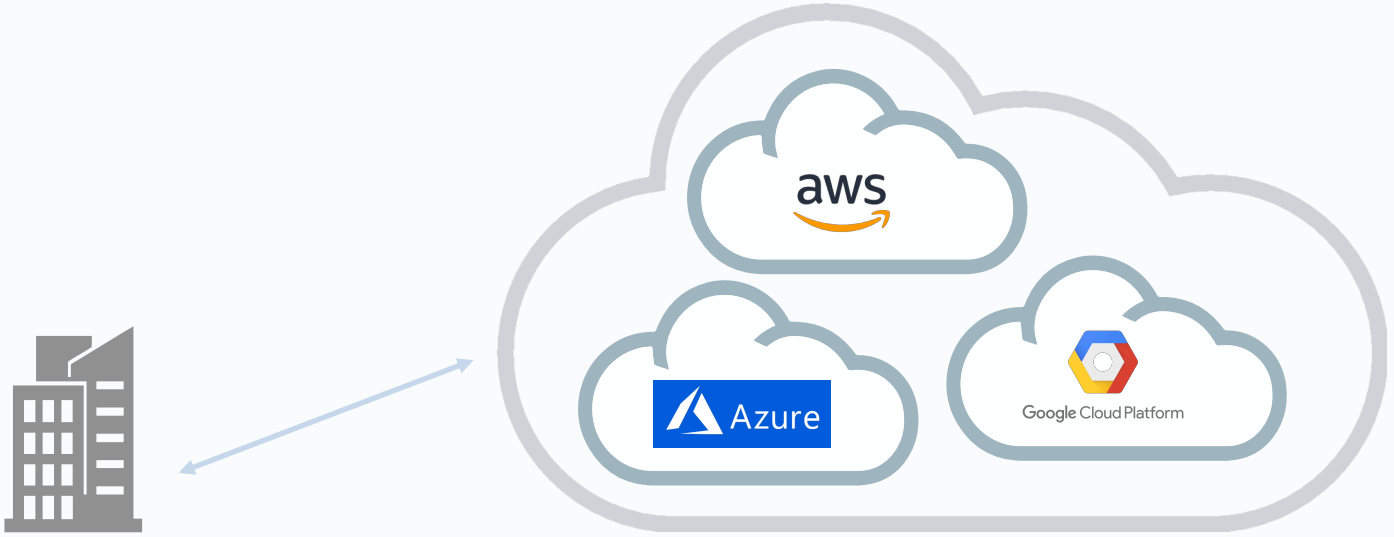


DevSecOps Engineer

Responsible for automating security checks and remediating viable security threats in development/ deployment practices

AUTOMATION & ACTIONABLE DATA ….

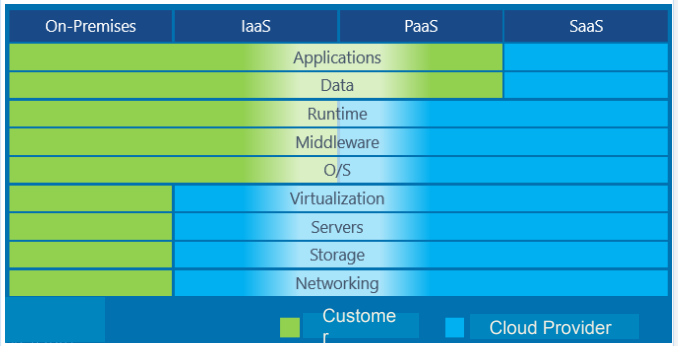
The New IT – Hybrid, Multi-Cloud Deployment



Shared Security Responsibility Model

You

are responsible for securing your data and workloads



Varies by layers

Image from Microsoft Azure Shared Security Responsibility

Qualys.

Securing Public Clouds Using Qualys

Customer Case Studies

Reduced application releases from 2 weeks to 24 hrs by automating security with Qualys in to DevOps

A SOFTWARE MAKER Private

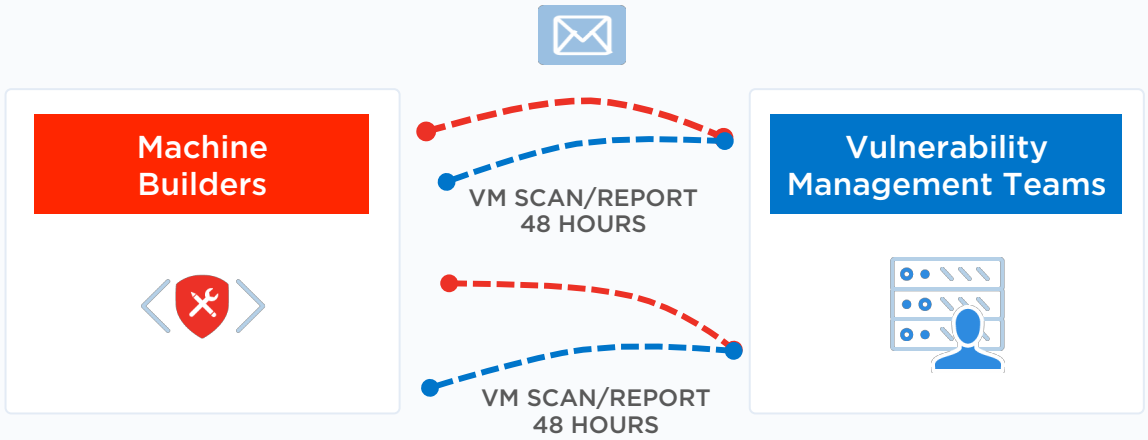
"Just in time" security approvals with end to End integration of Qualys Scan and Reports with Service Now,

A BEVERAGE MNC Private

Enabling DevOps with automated agent deployment via Azure Security Center

CapitalOne

Before: Lack of Security Automation Delays Release

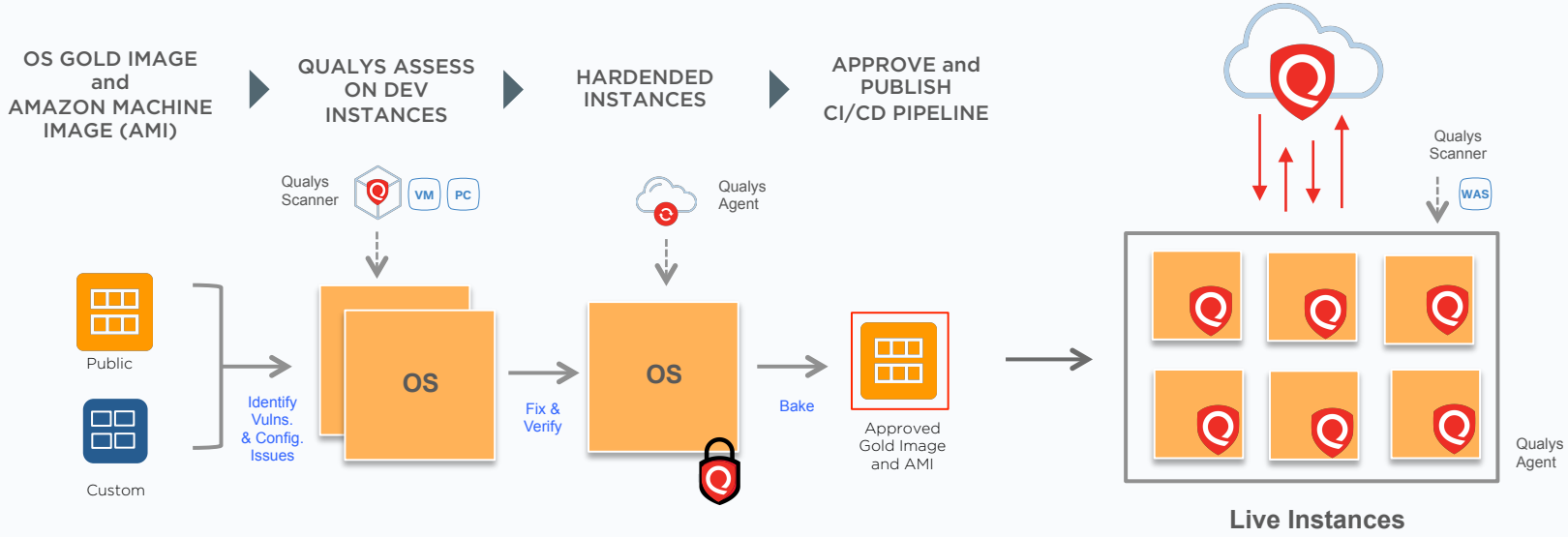


Two weeks until the Image (AMI) is certified for production

Capital One

Introducing Security at the Source Bake

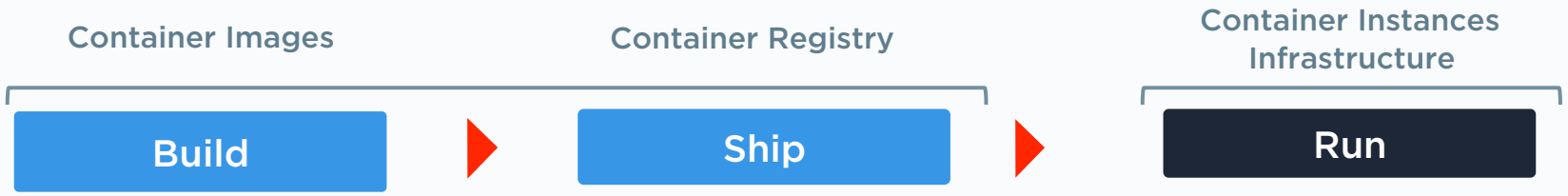
Qualys Security into Gold Images and AMI



Bakery process happens within 24 Hrs

Qualys.

Container Lifecycle Challenges



What's in the images?

Vulnerabilities?

OSS license exposure?

Solution disruptive to my CI Pipeline?

Scanning report integrated with bug tracking?

Registry scanning?

Enforce compliance?

Vulnerability, package and license-based rules?

Vulnerability impact notifications?

How to protect host?

Container engine configured correctly?

Container orchestration configured correctly?

Runtime app visibility?

Runtime app protection?

Qualys.

Qualys Container Security

Host Protection

CIS Benchmarks

Protection for container infrastructure stack

Scanning & Compliance

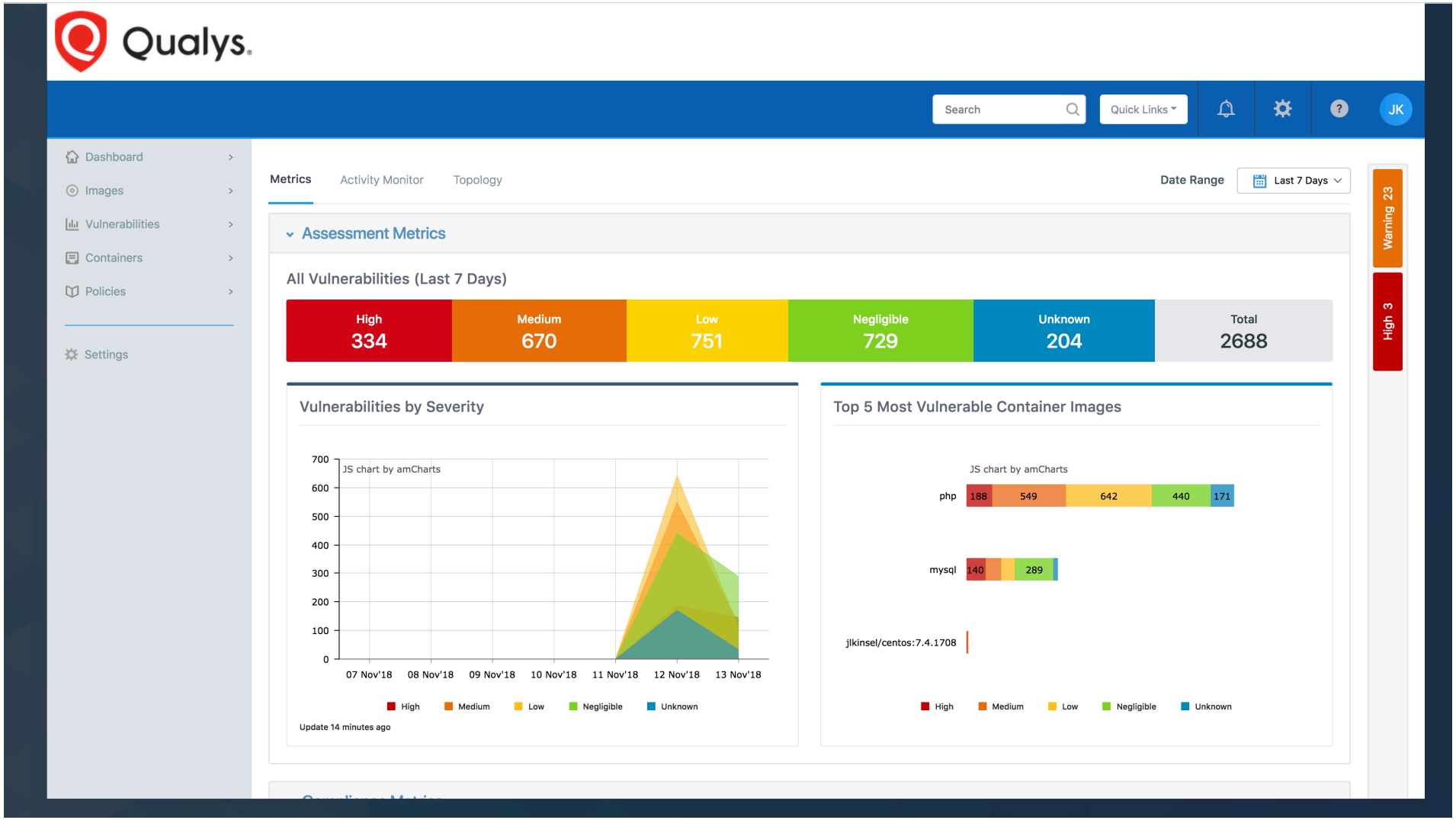
Accurate insight and control of container images

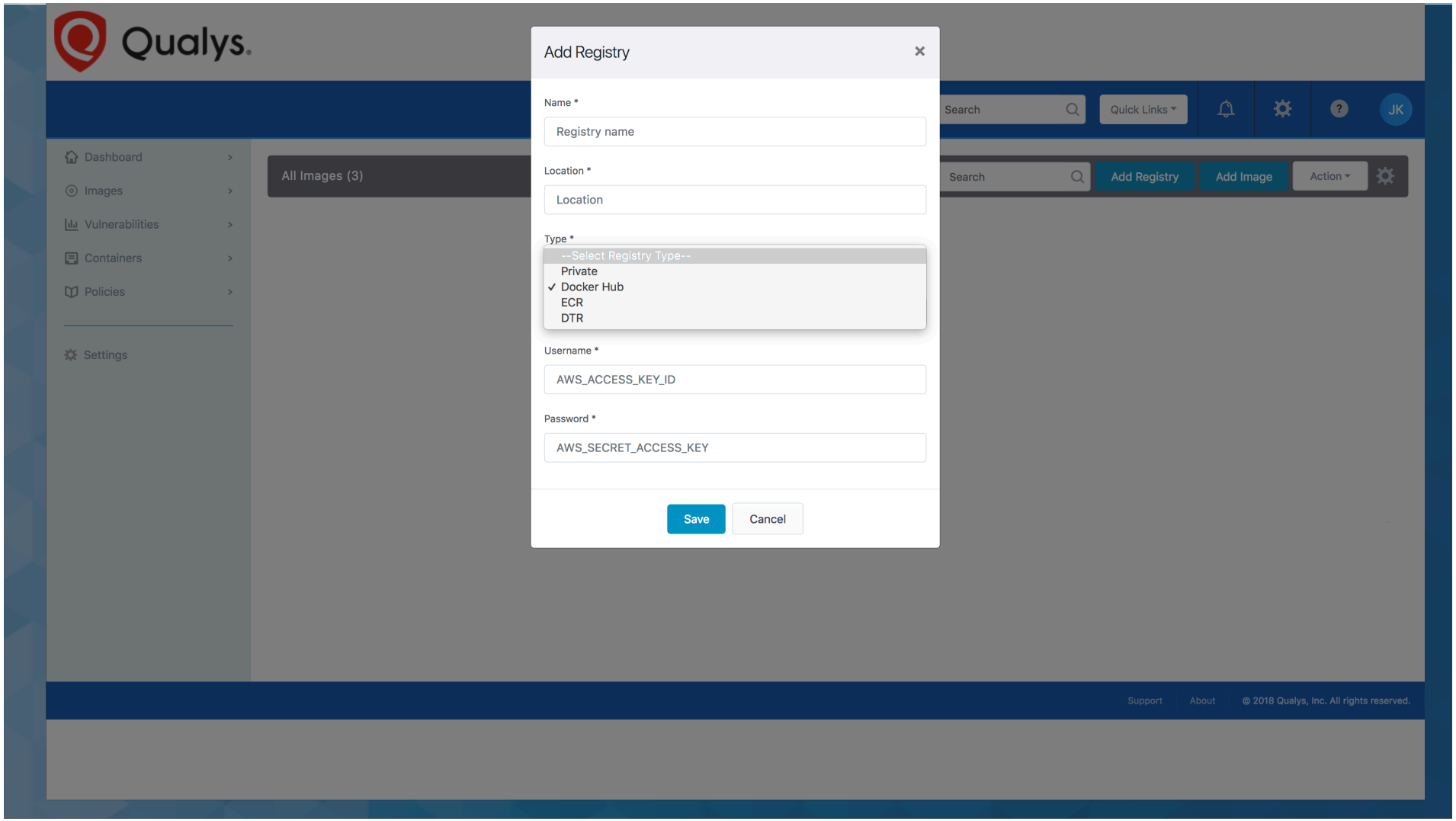
Visibility & Protection

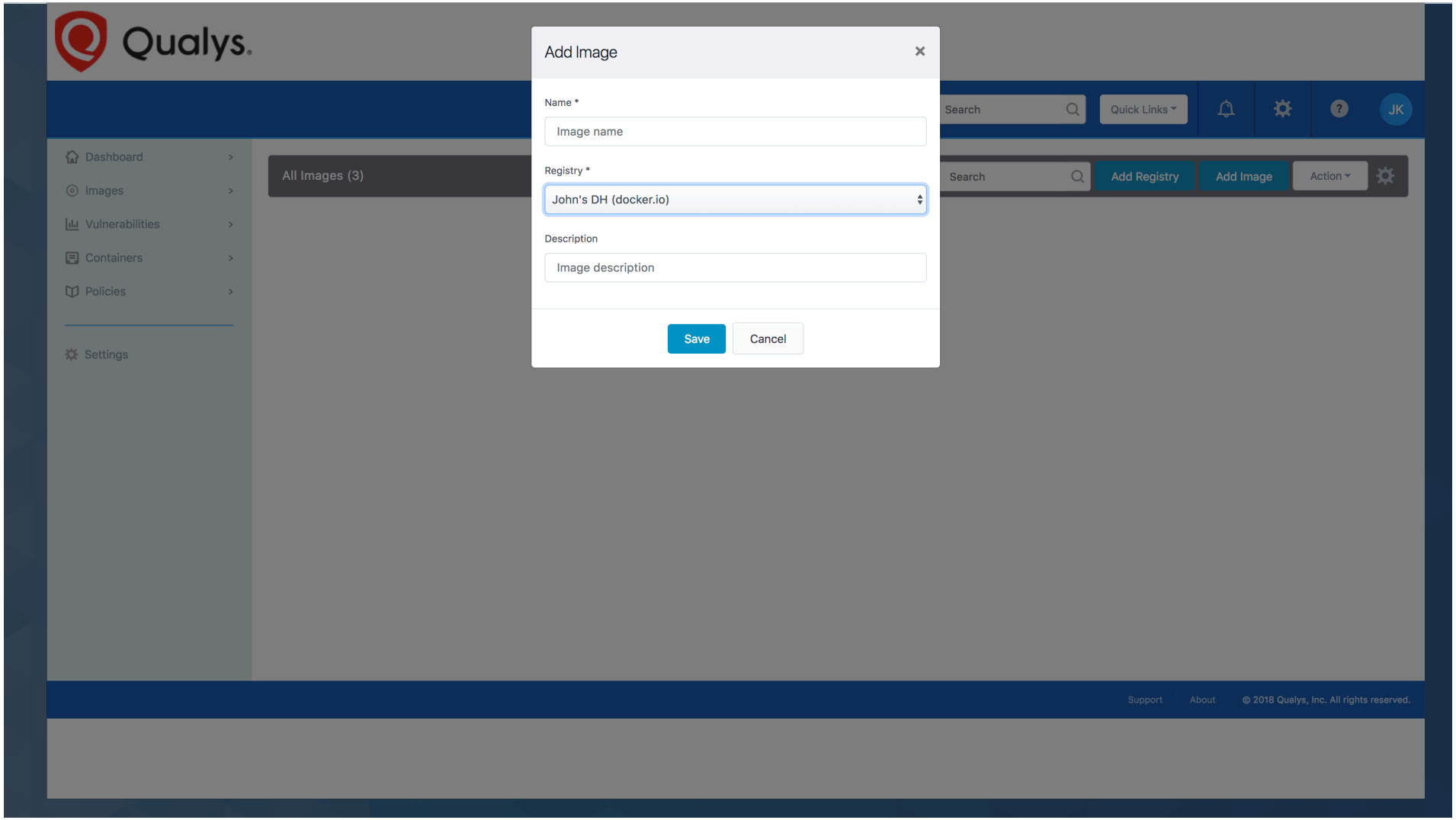
Automated analysis and enforcement of container behavior

Qualys.

Demo


Qualys.
Search
Quick Links
JK
Dashboard
Images
Vulnerabilities
Containers
Policies
Settings
Metrics
Activity Monitor
Topology
Date Range
Last 7 Days
Warning 23
High 3
Assessment Metrics
All Vulnerabilities (Last 7 Days)
High 334
Medium 670
Low 751
Negligible 729
Unknown 204
Total 2688
Vulnerabilities by Severity
JS chart by amCharts
700
600
500
400
300
200
100
0
07 Nov'18
08 Nov'18
09 Nov'18
10 Nov'18
11 Nov'18
12 Nov'18
13 Nov'18
High
Medium
Low
Negligible
Unknown
Update 14 minutes ago
Top 5 Most Vulnerable Container Images
JS chart by amCharts
php
188
549
642
440
171
mysql
140
289
jlkinsel/centos:7.4.1708
High
Medium
Low
Negligible
Unknown


Qualys.
Search
Quick Links
JK
Dashboard
Images
Vulnerabilities
Containers
Policies
Settings
All Images (3)
Search
Add Registry
Add Image
Action
Add Registry
Name *
Registry name
Location *
Location
Type *
--Select Registry Type--
Private
Docker Hub
ECR
DTR
Username *
AWS_ACCESS_KEY_ID
Password *
AWS_SECRET_ACCESS_KEY
Save
Cancel
Support
About
© 2018 Qualys, Inc. All rights reserved.


Qualys.
Search
Quick Links
JK
Dashboard
Images
Vulnerabilities
Containers
Policies
Settings
All Images (3)
Search
Add Registry
Add Image
Action
Add Image
Name *
Image name
Registry *
John's DH (docker.io)
Description
Image description
Save
Cancel
Support
About
© 2018 Qualys, Inc. All rights reserved.

Qualys.

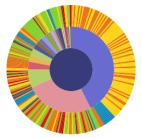
Search | Quick Links | JK

- Dashboard
- Images
- Vulnerabilities
- Containers
- Policies
- Settings

All Images (3)

Search | Add Registry | Add Image | Action

php
Scan Status: done
Instrumentation Status: Not Instrumented

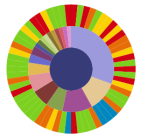


Actions

jlkinsel/centos:7.4.1708
Scan Status: done
Instrumentation Status: Active

Actions

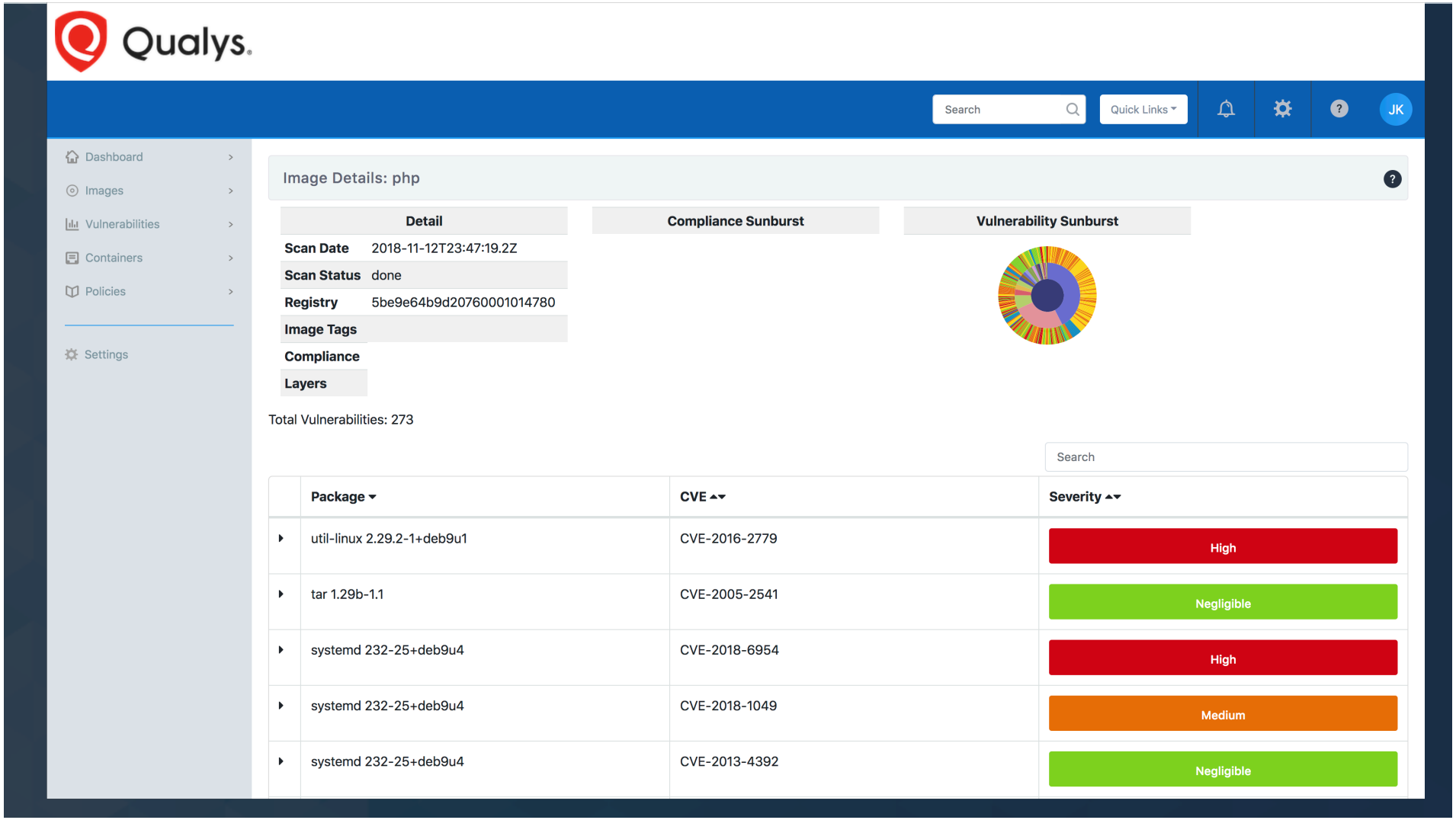
mysql
Scan Status: done
Instrumentation Status: Not Instrumented



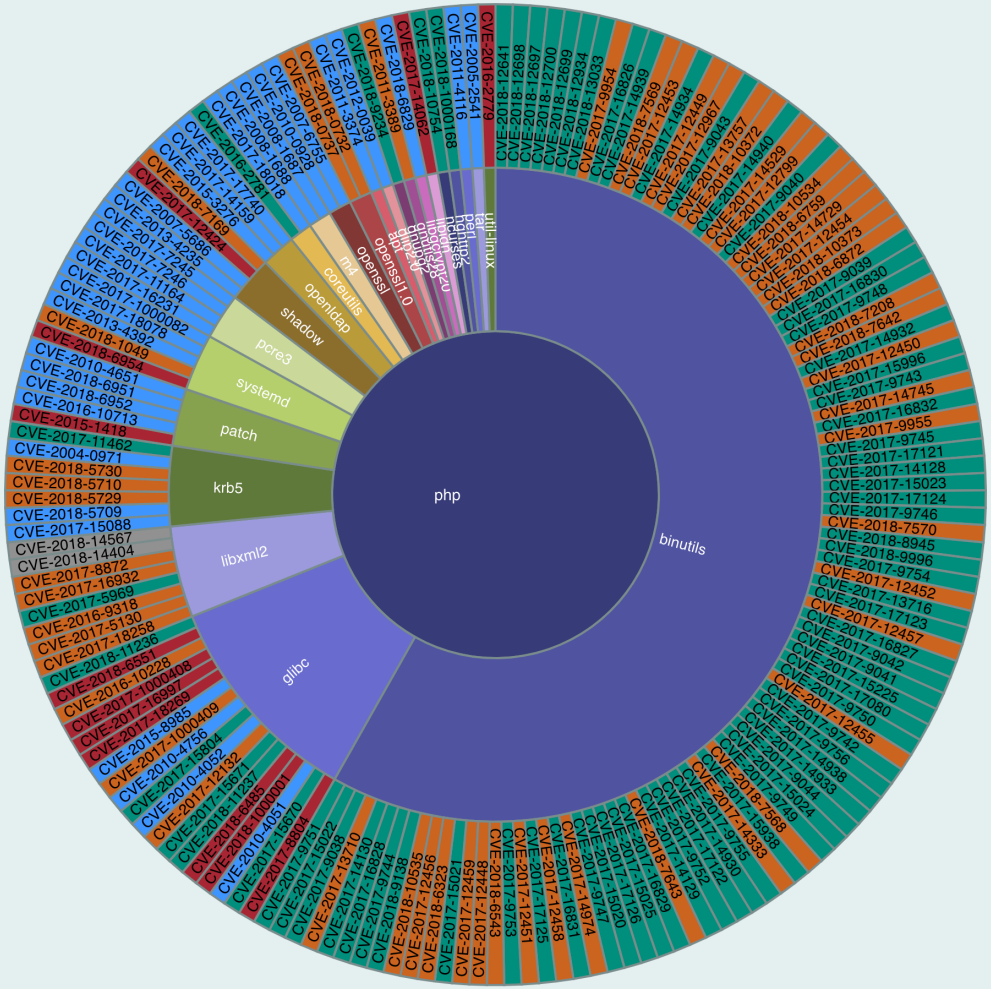
Actions

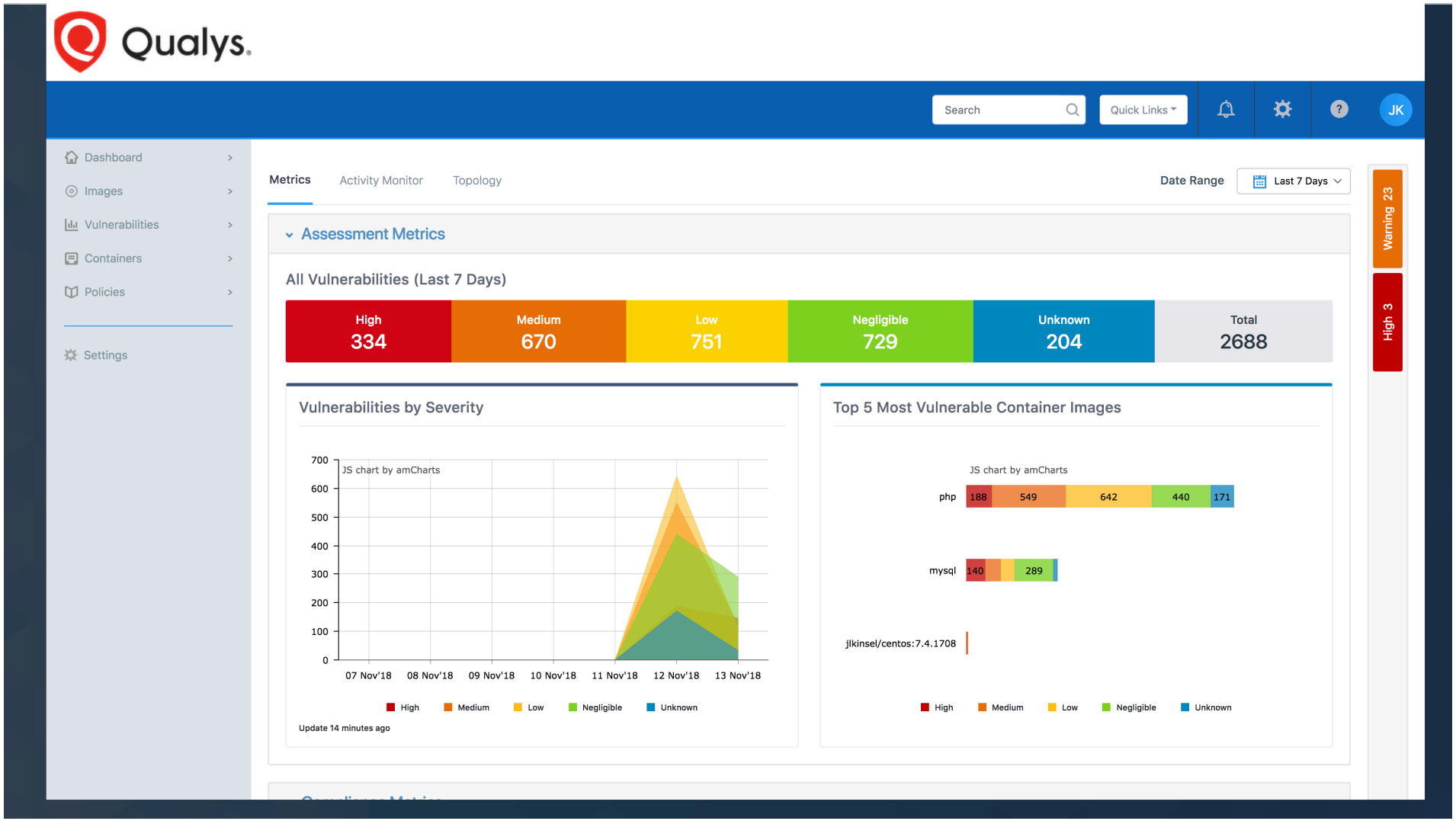
Records per page 10

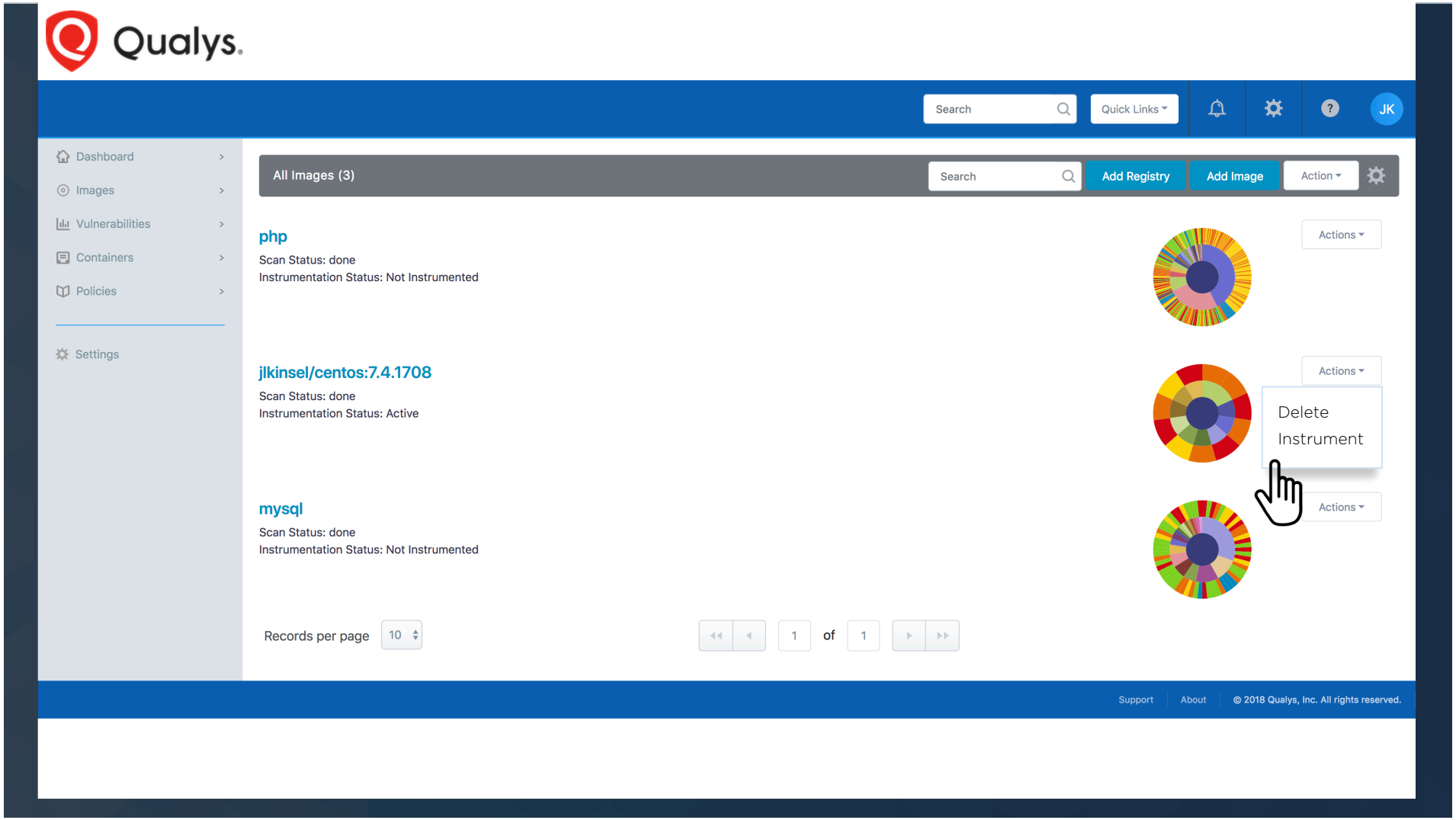
1 of 1

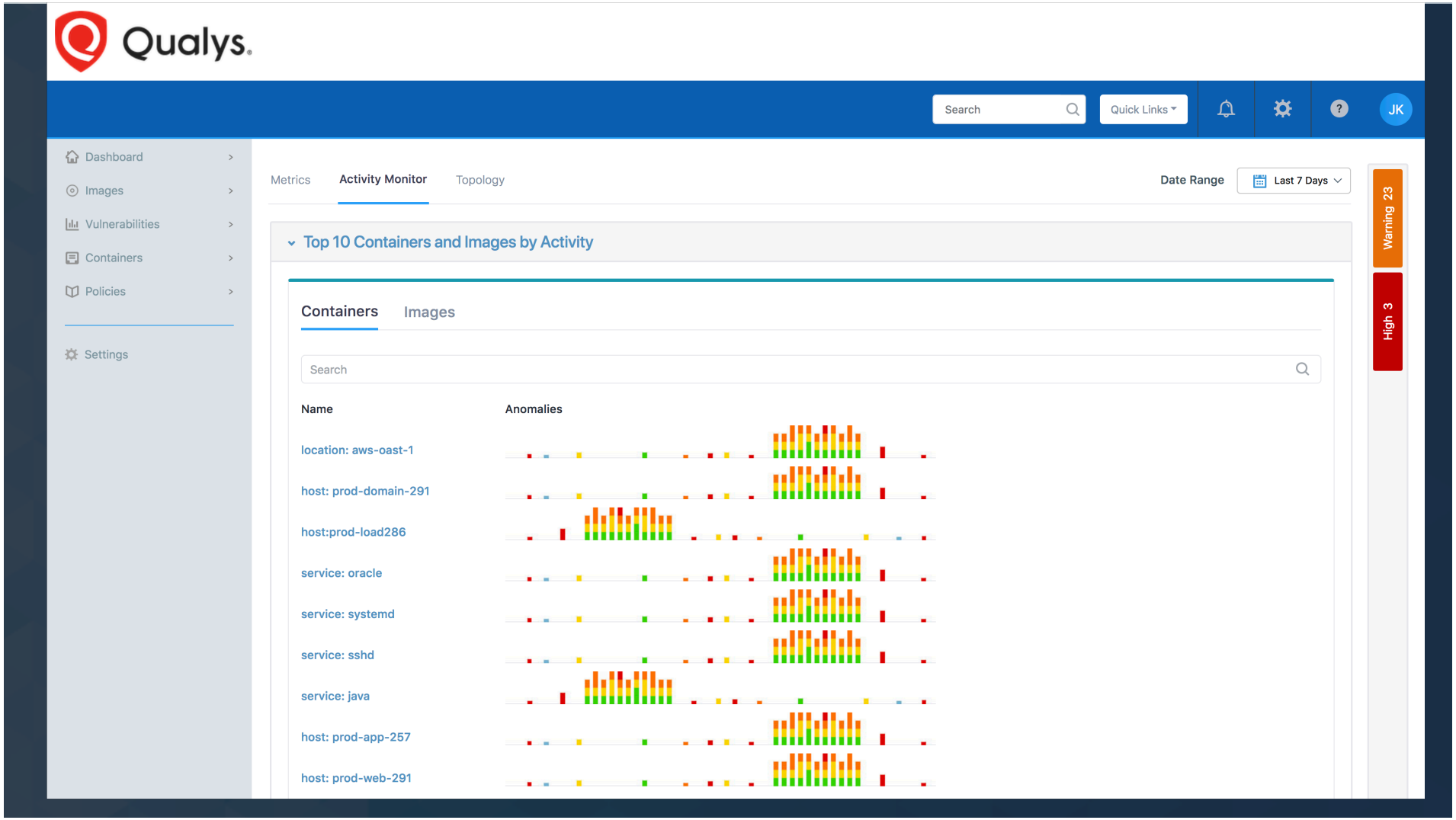

Qualys.
Search
Quick Links
JK
Dashboard
Images
Vulnerabilities
Containers
Policies
Settings
Image Details: php
Detail
Scan Date 2018-11-12T23:47:19.2Z
Scan Status done
Registry 5be9e64b9d20760001014780
Image Tags
Compliance
Layers
Compliance Sunburst
Vulnerability Sunburst
Total Vulnerabilities: 273
Search
Package
CVE
Severity
util-linux 2.29.2-1+deb9u1 CVE-2016-2779 High
tar 1.29b-1.1 CVE-2005-2541 Negligible
systemd 232-25+deb9u4 CVE-2018-6954 High
systemd 232-25+deb9u4 CVE-2018-1049 Medium
systemd 232-25+deb9u4 CVE-2013-4392 Negligible

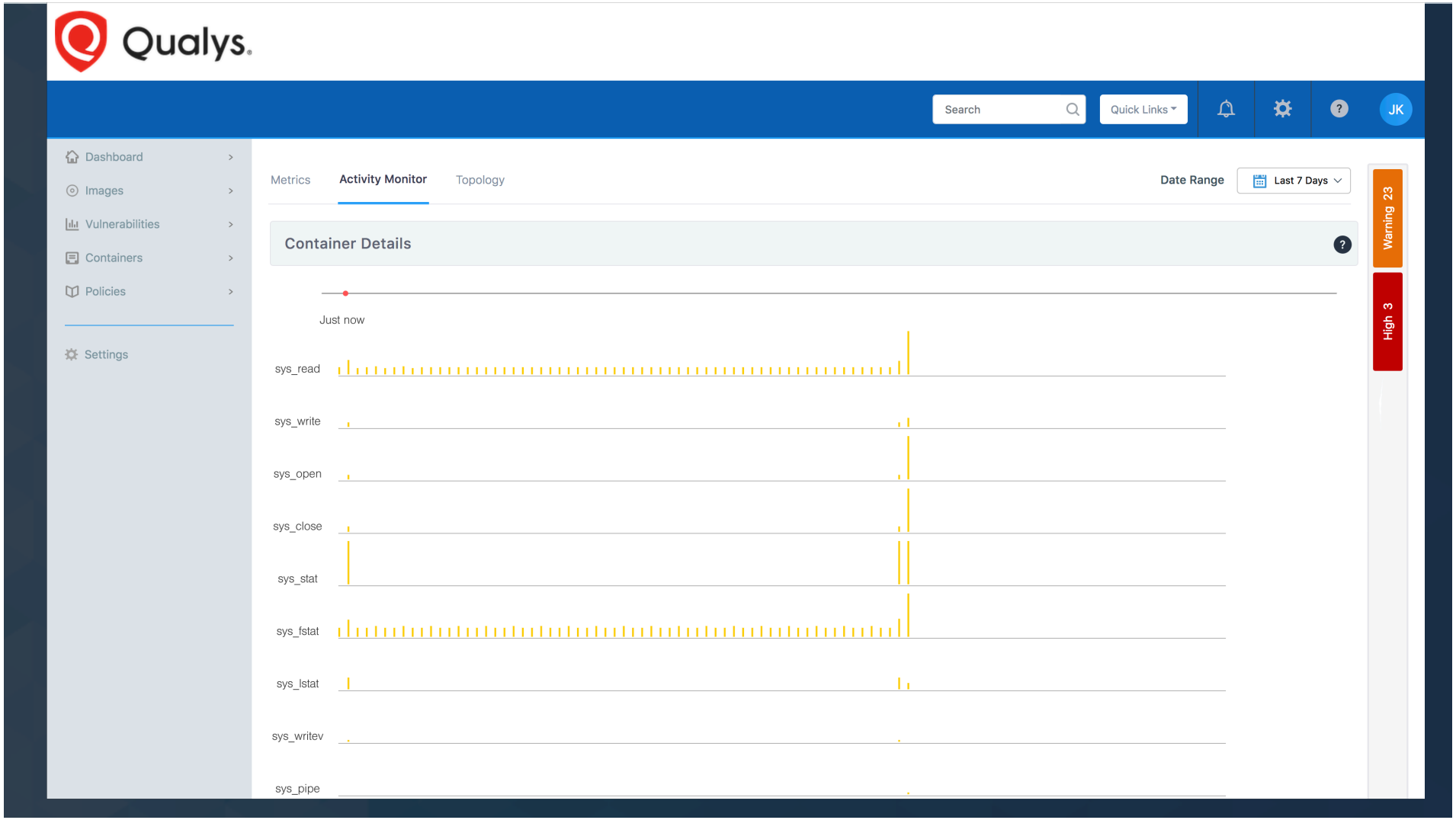
Vulnerability Sunburst of php

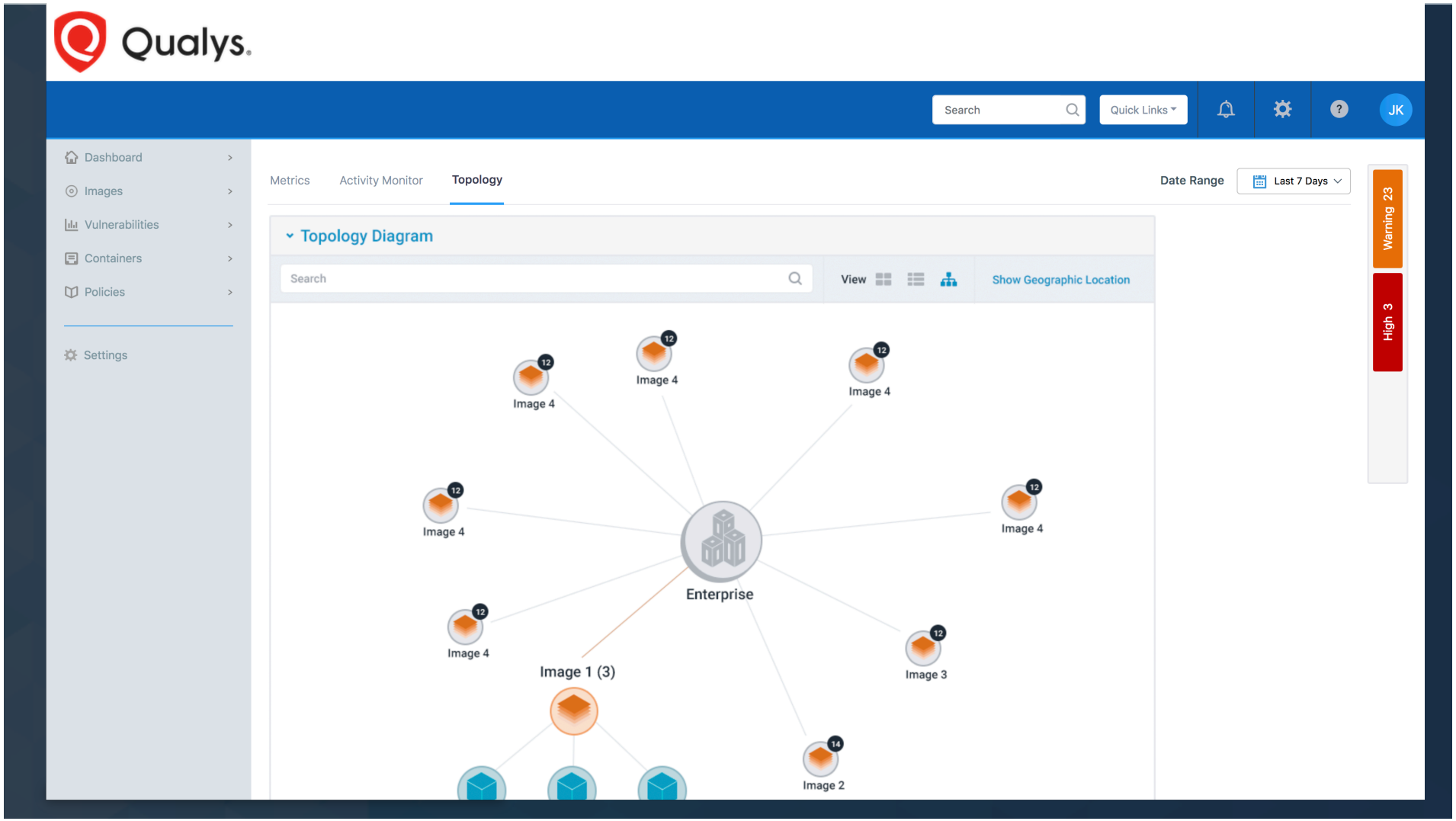


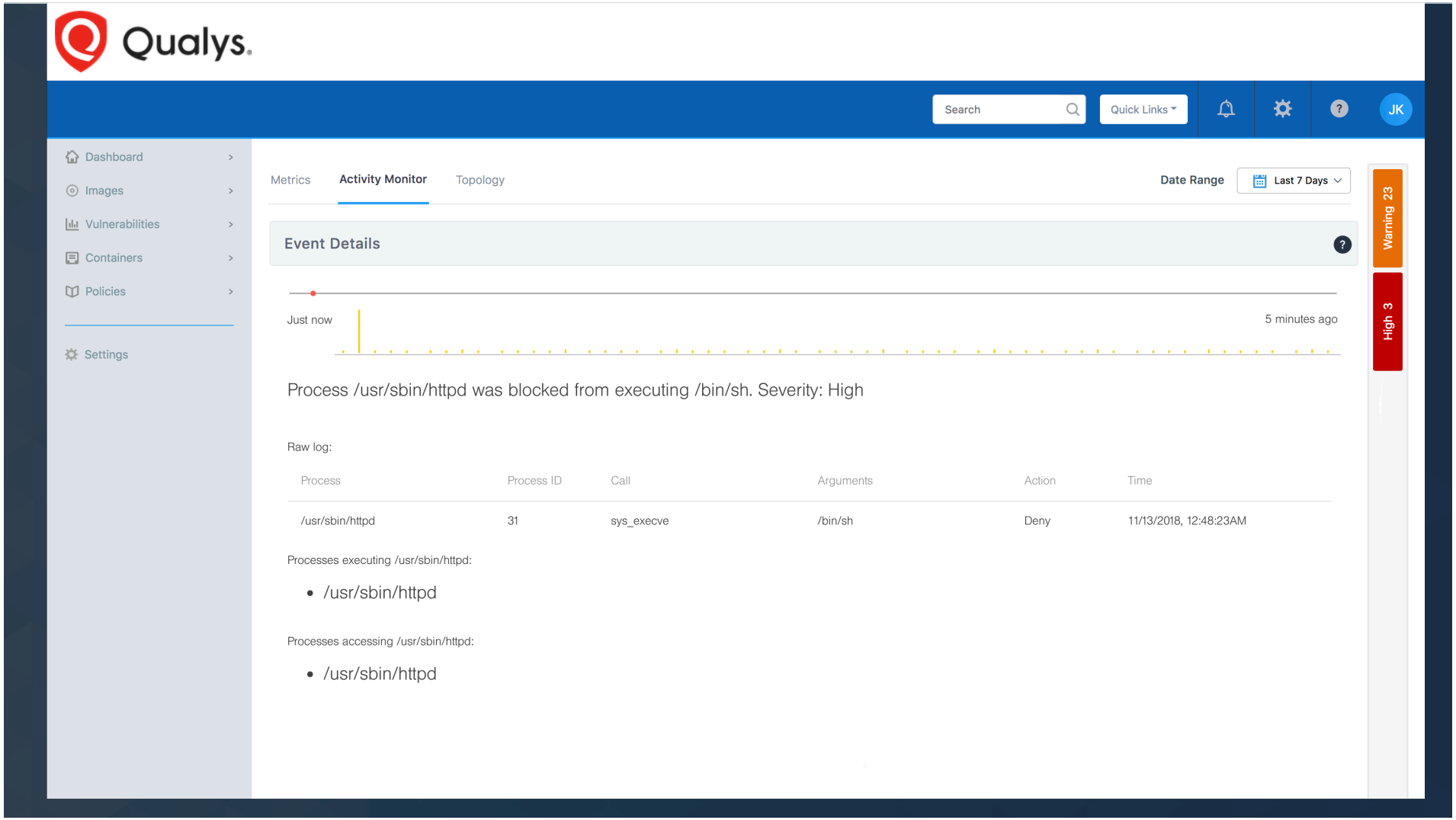

Qualys.
Search
Quick Links
JK
Dashboard
Images
Vulnerabilities
Containers
Policies
Settings
Metrics
Activity Monitor
Topology
Date Range
Last 7 Days
Warning 23
High 3
Assessment Metrics
All Vulnerabilities (Last 7 Days)
High 334
Medium 670
Low 751
Negligible 729
Unknown 204
Total 2688
Vulnerabilities by Severity
JS chart by amCharts
700
600
500
400
300
200
100
0
07 Nov'18
08 Nov'18
09 Nov'18
10 Nov'18
11 Nov'18
12 Nov'18
13 Nov'18
High
Medium
Low
Negligible
Unknown
Update 14 minutes ago
Top 5 Most Vulnerable Container Images
JS chart by amCharts
php
188
549
642
440
171
mysql
140
289
jlkinsel/centos:7.4.1708
High
Medium
Low
Negligible
Unknown

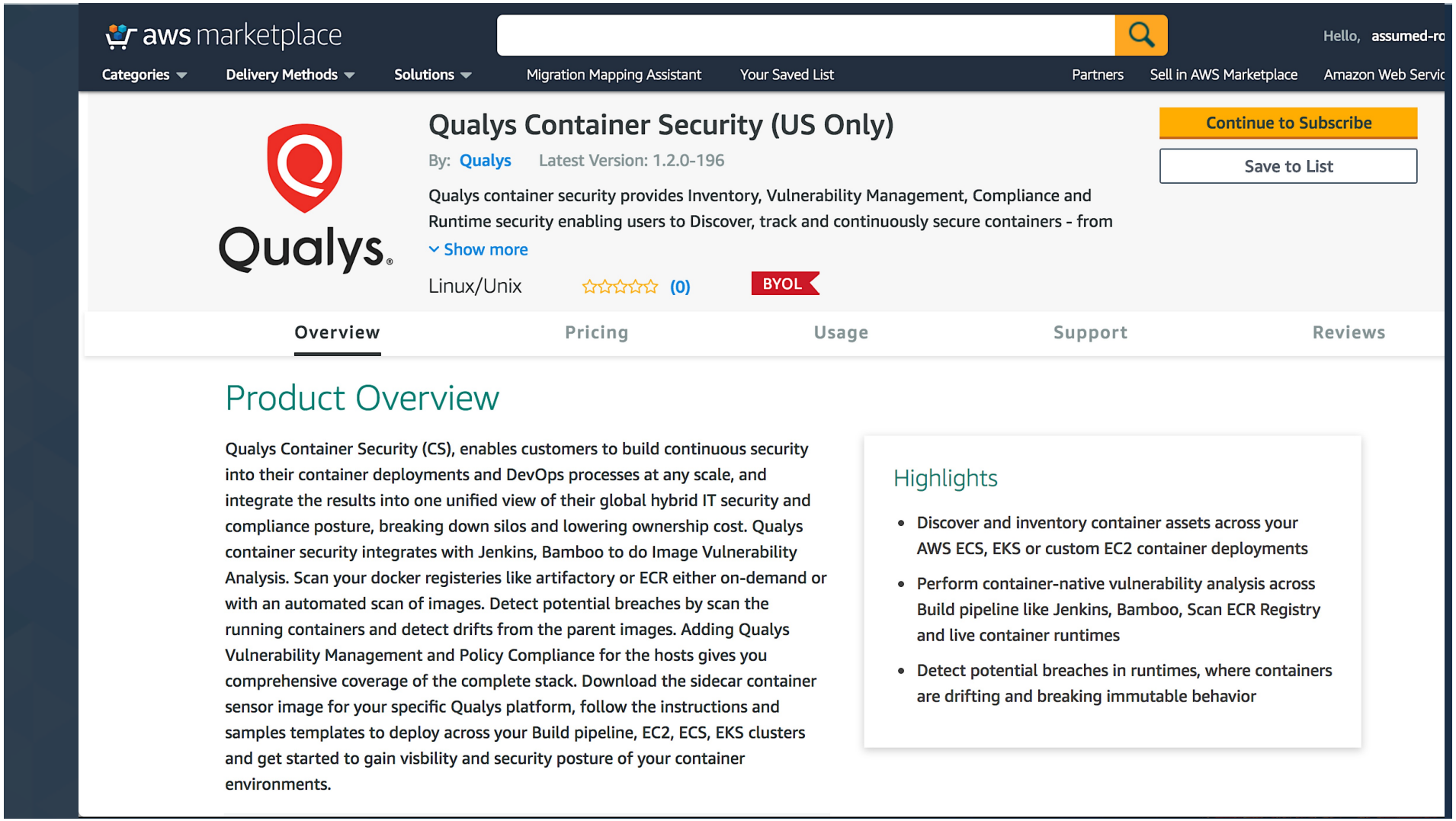

Qualys.
Search
Quick Links
JK
Dashboard
Images
Vulnerabilities
Containers
Policies
Settings
All Images (3)
Search
Add Registry
Add Image
Action
php
Scan Status: done
Instrumentation Status: Not Instrumented
Actions
jlkinsel/centos:7.4.1708
Scan Status: done
Instrumentation Status: Active
Actions
Delete Instrument
mysql
Scan Status: done
Instrumentation Status: Not Instrumented
Actions
Records per page
10
1
of
1
Support
About
© 2018 Qualys, Inc. All rights reserved.


Qualys.
Search
Quick Links
JK
Dashboard
Images
Vulnerabilities
Containers
Policies
Settings
Metrics
Activity Monitor
Topology
Date Range
Last 7 Days
Warning 23
High 3
Top 10 Containers and Images by Activity
Containers
Images
Search
Name
Anomalies
location: aws-oast-1
host: prod-domain-291
host:prod-load286
service: oracle
service: systemd
service: sshd
service: java
host: prod-app-257
host: prod-web-291


Qualys.
Search
Quick Links
JK
Dashboard
Images
Vulnerabilities
Containers
Policies
Settings
Metrics
Activity Monitor
Topology
Date Range
Last 7 Days
Warning 23
High 3
Container Details
Just now
sys_read
sys_write
sys_open
sys_close
sys_stat
sys_fstat
sys_lstat
sys_writev
sys_pipe


Qualys.
Search
Quick Links
JK
Dashboard
Images
Vulnerabilities
Containers
Policies
Settings
Metrics
Activity Monitor
Topology
Date Range
Last 7 Days
Warning 23
High 3
Topology Diagram
Search
View
Show Geographic Location
Image 4
Image 4
Image 4
Image 4
Image 4
Image 4
Enterprise
Image 1 (3)
Image 3
Image 2


Qualys.
Search
Quick Links
JK
Dashboard
Images
Vulnerabilities
Containers
Policies
Settings
Metrics
Activity Monitor
Topology
Date Range
Last 7 Days
Warning 23
High 3
Event Details
Just now
5 minutes ago
Process /usr/sbin/httpd was blocked from executing /bin/sh. Severity: High
Raw log:
Process
Process ID
Call
Arguments
Action
Time
/usr/sbin/httpd
31
sys_execve
/bin/sh
Deny
11/13/2018, 12:48:23AM
Processes executing /usr/sbin/httpd:
/usr/sbin/httpd
Processes accessing /usr/sbin/httpd:
/usr/sbin/httpd


aws marketplace
Hello, assumed-ro
Categories
Delivery Methods
Solutions
Migration Mapping Assistant
Your Saved List
Partners
Sell in AWS Marketplace
Amazon Web Servic
Qualys Container Security (US Only)
By: Qualys
Latest Version: 1.2.0-196
Qualys container security provides Inventory, Vulnerability Management, Compliance and Runtime security enabling users to Discover, track and continuously secure containers - from
Show more
Linux/Unix
(0)
BYOL
Continue to Subscribe
Save to List
Overview
Pricing
Usage
Support
Reviews
Product Overview
Qualys Container Security (CS), enables customers to build continuous security into their container deployments and DevOps processes at any scale, and integrate the results into one unified view of their global hybrid IT security and compliance posture, breaking down silos and lowering ownership cost. Qualys container security integrates with Jenkins, Bamboo to do Image Vulnerability Analysis. Scan your docker registeries like artifactory or ECR either on-demand or with an automated scan of images. Detect potential breaches by scan the running containers and detect drifts from the parent images. Adding Qualys Vulnerability Management and Policy Compliance for the hosts gives you comprehensive coverage of the complete stack. Download the sidecar container sensor image for your specific Qualys platform, follow the instructions and samples templates to deploy across your Build pipeline, EC2, ECS, EKS clusters and get started to gain visbility and security posture of your container environments.
Highlights
Discover and inventory container assets across your AWS ECS, EKS or custom EC2 container deployments
Perform container-native vulnerability analysis across Build pipeline like Jenkins, Bamboo, Scan ECR Registry and live container runtimes
Detect potential breaches in runtimes, where containers are drifting and breaking immutable behavior

Thank You

Leif Kremkow
LKremkow@qualys.com